Risk Modeling, Assessment, and Management of Interdependent Critical Infrastructures

Professor Yacov Y. Haimes, Professor James H. Lambert
Mr. Brian B. Mahoney

Center for Risk Management of Engineering Systems
University of Virginia

16th Annual Security Technology Symposium
Williamsburg, VA
29 June 2000

Agenda

- **Background**
- **Guiding Principles for Holistic Risk Management**
- **Survey of Systems Engineering Tools and Methodologies, and Modeling Techniques**
- **Modeling the Complexity of Interdependent Infrastructures**
- **R&D, Educational, and Training Dimension**
- **Epilogue**
- **Backup Material**
  - **References for Tools and Methods**

Background

- UVA's Risk Center Involvement with Infrastructure Protection began with President Commission on Critical Infrastructure Protection
- Current Infrastructure Assurance work is primarily supported by DoD's Joint Program Office/Infrastructure Assurance (JPO/IA) located at the Naval Surface Warfare Center, Dahlgren, VA
  - Research and benchmark best risk management practices from Fortune 500 corporations
- Active liaison with the Office of Science and Technology Policy
- Additional related research is also being supported by the National Ground Intelligence Center and NASA Langley

Guiding Principles for a Holistic Risk Management

The essence of any decision-making, whether at the family level, the corporate level, or the governmental level is making trade-offs among very difficult and complex objectives (such as cost, benefit, and risk) that are often in conflict and competition with one another.

- Risk Assessment and management should employ a holistic, multi-objective framework
- Good quantitative risk assessment and management must be grounded on basic systems engineering philosophy and principles.
- A comprehensive risk assessment must be grounded on a holistic search of all critical sources of risk.
- Risk and safety are two different, albeit related, entities.
- To the extent that risk assessment is precise, it is not real.
- To the extent that risk assessment is real, it is not precise.

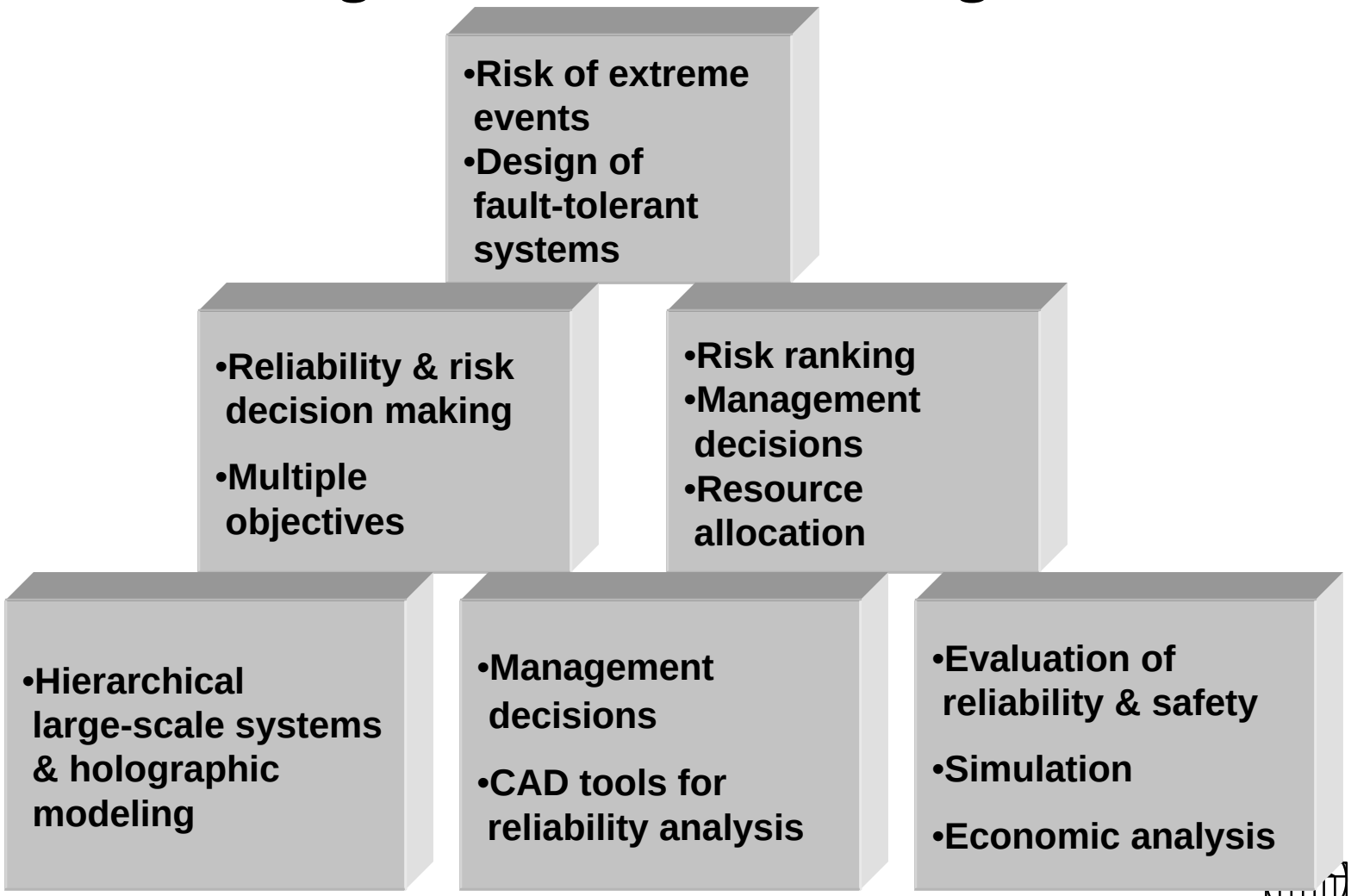
Risk versus Safety

- Risk - The measure of probability and severity of adverse effects.

- Safety - Who should decide on the acceptability of what risks, under what terms, and why?

(Lowrance, 1976)

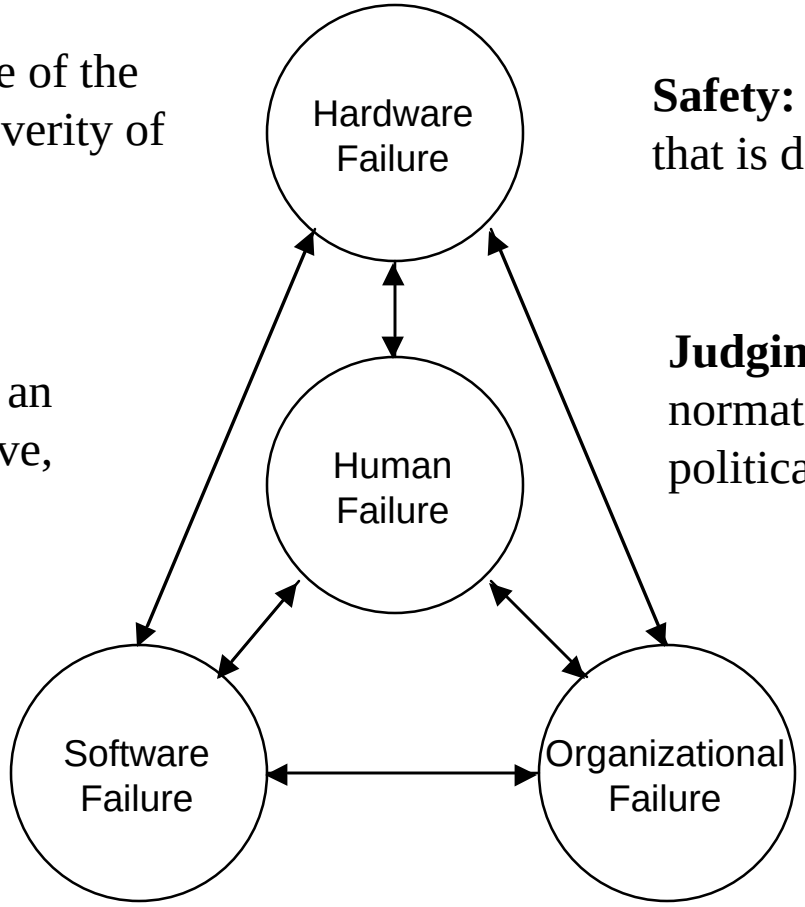
Building Blocks of Risk Management



Major Sources of System Failure

Risk: is a measure of the probability and severity of adverse effects

Measuring Risk: is an empirical, quantitative, scientific activity



Safety: is the level of risk that is deemed acceptable

Judging safety: is a normative, qualitative, political activity

(W.W. Lowrance, 1976)

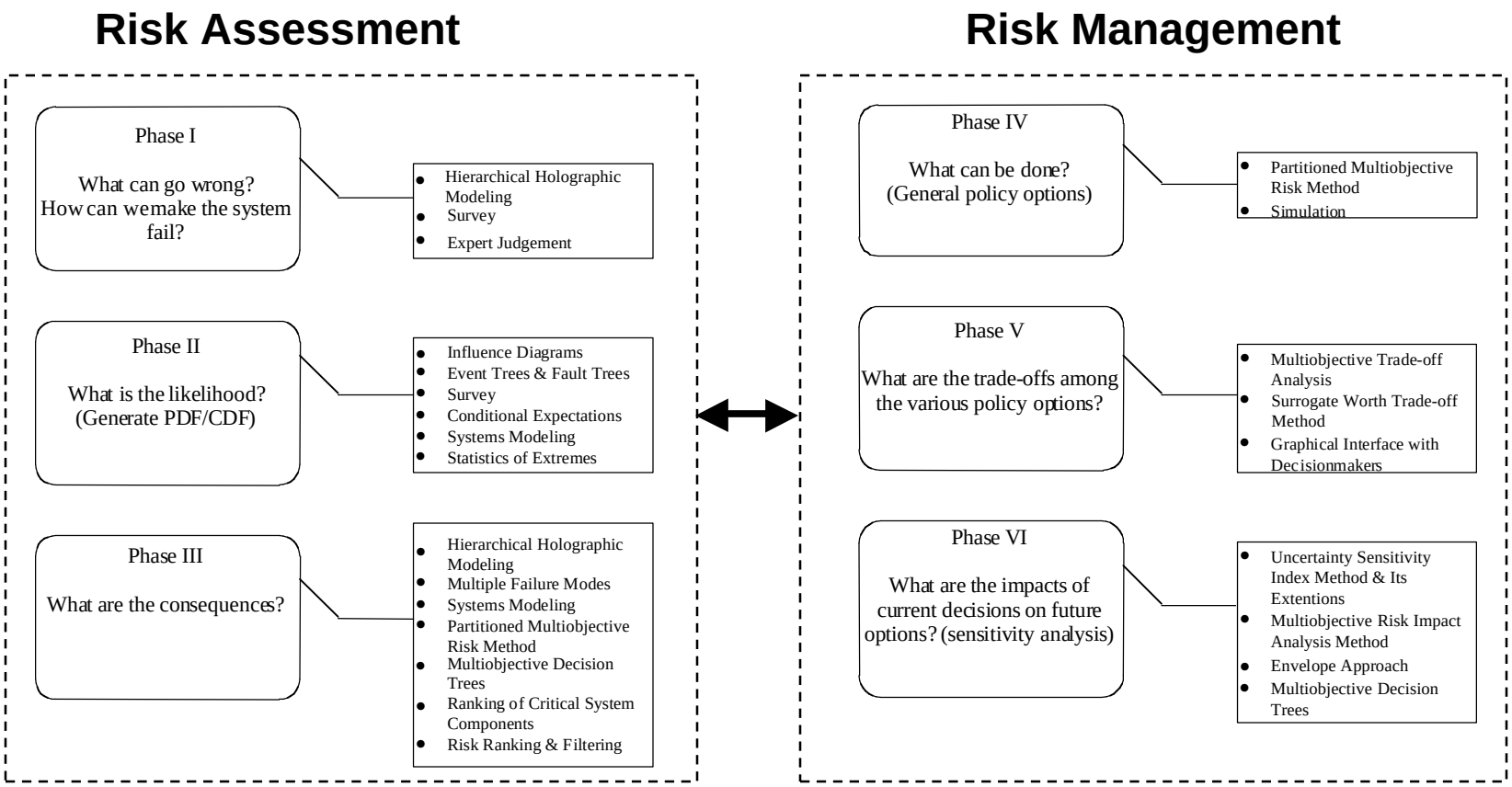
The Importance of Considering the Four Sources of Failure

- First, they are comprehensive, addressing all aspects of the infrastructures' planning, design, construction, operation, and management.

- Secondly, they require the total involvement in the risk assessment and management process of everyone concerned – blue/white collar workers and managers at all levels of the organizational hierarchy.

- Thirdly, they dramatize the equal importance of human and especially organizational failures.

Framework for Risk Assessment and Management



Sample Case Studies in Multi-objective Risk Management

1. **Risk Management Support for Operations Other Than War**
2. **Risk Ranking for Space Shuttle and Space Station**
3. **Dam Safety**
4. **Flood Warning and Evacuation Systems**
5. **Vulnerability of Critical Physical Infrastructures**
6. **Reliability-Based Management of the Navigation System in the Upper Mississippi River**
7. **Holistic Risk Management for Software Acquisition**
8. **Evaluation of Automobile Safety Features in a Multi-objective Risk Framework**
9. **Multi-objective decision making for Flood Plain Management**
10. **Holographic Reliability Modeling for Water Distribution Rehabilitation**
11. **Critical Infrastructure Protection of Water Supply Systems**

Survey of Systems Engineering Tools and Methodologies, and Modeling Techniques

- **Different forms of describing success scenarios**
  - PERT, CPM, Gantt, etc.
  - CASE, OOD, etc.
  - Balance sheet, cash flow diagram, etc
  - Flow diagram
  - Process flow
  - Fault/ Event trees
  - Networks
  - Feedback control
  - Dynamic system

Modeling the Effects of Events on the Success Scenario

- **Events in the real system can be modeled as changes in the success scenario model, for example**
  - Change a parameter value
  - Remove a component
  - Degrade a component
  - Change the rules of interaction
  - Change the environment
  - Defective component installation
  - Software mistake
  - Others

Applying Risk Management

- **Once the processes involved with entity are understood, the appropriate risk management tools can be associated with each process**
- **For example**
  - Multi-objective tradeoff analysis
  - Generation of Alternatives
- **Options for adding**
  - Robustness
  - Resiliency
  - Redundancy
- **Mission selection component**
- **Risk detection, prevention, and correction**

A taxonomy for tools and methods is being developed to evaluate available risk assessment and management methodologies

Taxonomy Topics

- **Automated software tools addressing Safety, Risk, or Reliability Analysis**
  - e.g., @Risk, Buddy, Galileo, BARP, RISKMAN, Faultrease
- **Reliability tools and methods**
  - e.g., FMEA, FMECA, HAZOP, Fault Trees
- **General analytic risk tools and methods**
  - e.g., PMRM, AFD, HHM, SOFIA
- **Domain specific tools and methods**
  - e.g., Nuclear, Transportation, Water, Space, Medical
- **General engineering and project management tools and methods**
  - e.g., PERT, Gantt, CPM, Earned-value, Simulation and Modeling, SEI-CMM

Acronyms/Definitions

AFD	–	Anticipatory Failure Determination
BARP	–	Bayesian Reliability Program
CASE	–	Computer Aided Systems Engineering
FMEA	–	Failure Modes and Effects Analysis
FMECA	–	Failure Modes Effects and Criticality Analysis
HAZOP	–	Hazard and Operation Analysis
OOD	–	Object Oriented Design
PMRM	–	Partitioned Multi-objective Risk Method
SOFIA	–	Simulation Object Framework for Infrastructure Analysis
SEI-CMM	–	Software Engineering Institute – Capability Maturity Model

Sources of Information

- **Gather tools and methods from:**
  - Review of literature
  - Contact with leading industry representatives
  - Other universities
  - Federally sponsored research institutes
- **Continue to explore relationships with industry contacts to maintain balance between academic and business tools and methods**

Taxonomy Mapping

- Taxonomy tools and methods will be mapped to the “six questions” of risk assessment and management
- A tool may support a particular aspect or the entire life cycle of risk assessment and management

Modeling the Complexity of Interdependent Infrastructures

Challenges and Opportunities in the Protection of the Nation's Critical Interdependent Infrastructures

Modeling and Educational Dimensions

Modeling the Complexity of Interdependent Infrastructures

Characteristics of the multifarious nature of independent infrastructures:

- large-scale systems of systems with numerous components,
- hierarchical multiple non-commensurable, conflicting and competing objectives,
- multiple agents and decision-makers,
- multiple agencies with different missions, resources, timetables, and agendas,
- multiple constituencies,
- multiple transcending aspects and functions,
- nonlinear coupled subsystems,
- spatially distributed, adaptive,
- organizational and human errors and failures are common, and
- managing risk and uncertainty associated with extreme and catastrophic events are of paramount importance.

Information Assurance and Its Impact on Interdependencies

- The complexity of our technological society has forced us to deal with coupled and interconnected "systems of systems" whose likelihood of serious disruptions whether accidental or intentional are increasing.
- In addressing the role of information assurance (IA) in the protection of interconnected infrastructures, it is important to recognize the difference between information technology (IT) and IA.
- Whereas IT is fundamentally a generic technology-based entity, which connotes the development and deployment of hardware and software, IA is an integrated technology/people/organizational-based entity, with trustworthiness as its hallmark.
- IT can be viewed as a subset of IA.
- The trustworthiness of IA necessitates an in-kind approach in the vision and mission of our research and development on the interdependencies of infrastructures.

Trustworthiness and Information Assurance

- The element of trust is the key ingredient for IA, and thus for the survivability and integrity of our critical infrastructures.

- The ever-increasing use of supervisory control and data acquisition (SCADA) systems for the remote operation of an infrastructure through the telecommunications network, has rendered our critical infrastructures more vulnerable to intrusion, and to the transmission of malicious misinformation and signals.

- Because science and engineering alone cannot achieve trustworthiness in the integrity of information transmission, IA requires the contributions of multiple disciplines that extend beyond science and engineering into the social and behavioral sciences, business, and law.

Modeling the Complexity of Interdependent Infrastructures

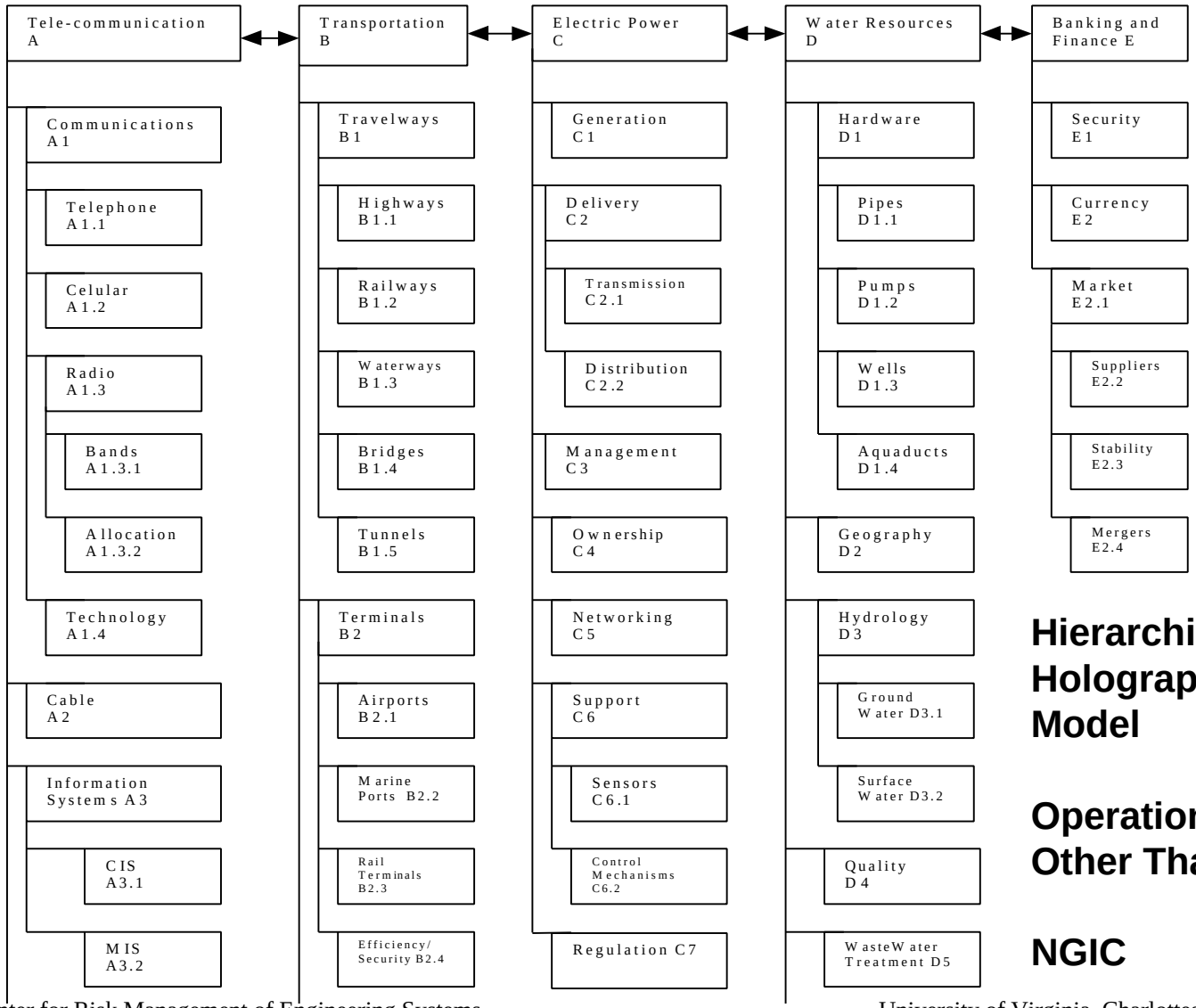
- Good quantitative risk assessment and management of interdependent infrastructures must be grounded on basic holistic systems engineering philosophy and principles.
- There is a need to develop a holistic methodological framework for understanding, modeling, and assessing the risks facing critical intra- and interdependent civilian and defense infrastructures and for assuring their continued operation.
- Hierarchical holographic modeling (HHM) is one methodology that enables us to identify most (if not all) sources of risk. This holistic framework offers multiple visions and perspectives, which add strength to a system analysis (in this case, the complex defense and civilian infrastructures).
- HHM has been extensively and successfully deployed to study risks for government agencies such as the PCCIP, FBI, NASA, Virginia Department of Transportation (DOT), and the National Ground Intelligence Center, among others.

Hierarchical Holographic Modeling (HHM)

- The HHM methodology/philosophy is grounded on the premise that in the process of modeling large-scale and complex systems, more than one mathematical or conceptual model is likely to emerge.
- Each of these models may focus on a specific aspect, yet all may be regarded as acceptable representations of the infrastructure system.
- Therefore, it is impracticable to represent within a single model all the important and critical aspects of such systems, and a new approach is needed.
- Through HHM, multiple models can be developed and coordinated to capture the essence of the many dimensions, visions, and perspectives of infrastructure systems.

Attributes of HHM

- Provides a holographic view of a modeled system, and is thus, capable of identifying most if not all sources of risk
- Adds robustness and resilience to modeling by capturing various system aspects and other societal elements
- Provides more defined responsiveness in modeling development to available data so that different holographic models can make use of different databases
- Adds more realism to the entire modeling process by recognizing that the limitations of modeling complex systems via a single model are circumvented by a model that addresses specific aspects of the system
- Provides more responsiveness to the inherent hierarchies of multiple objectives/sub-objectives and multiple decision-makers associated with large-scale and complex systems



Hierarchical Holographic Model

Operations Other Than War

NGIC

R&D, Educational, and Training Dimension

The Educational Dimension of Infrastructure Protection

- All four major sources of system failures:
  - hardware,
  - software,
  - organizational, and
  - human (people)

  have their genesis in the lack of appropriate education and training.

- The quality of education and training of personnel affect the entire life cycle of all infrastructures whether at the conception, planning, architectural design and specification, construction, operation, maintenance, replacement, or modification.

The Educational Dimension of Infrastructure Protection (concluded)

- In the US free-market economy, this truism has a most fundamental impact on the ability of the nation to realize its vision and goal of ensuring that our critical interdependent infrastructures remain resilient and able to withstand willful attacks.

- There are myriad conditions that influence and determine the number and the educational and training levels of the technical personnel who would ultimately commit themselves to fulfill the many functions in the life cycle of infrastructures.

- Paramount among these conditions are the opportunity for financial, and professional and personal growth made available to the educated and trained personnel, as well as the incentives provided for graduate students who would forgo substantial immediate income for future rewards by earning a master's or a Ph.D. degree.

The State of Research and Development and Graduate Level Education

- "Research and development are not presently adequate to support infrastructure protection." [PCCIP,1997: p. 23].

- "The shortage of workers with adequate skills makes it difficult for companies to grow both near and long-term research, even if budgets allowed. This alone suggests the critical need for additional government support of university research." [*Information Technology Research: Investing in Our Future*, The President's Information Technology Advisory Committee (PITAC), 1999].

- "When university researchers make an important basic discovery, they and their colleagues immediately increase their efforts along similar lines to confirm and amplify the discovery." [*America's Basic Research: Prosperity Through Discovery*, Committee for Economic Development, 1998, p.18].

The State of Research and Development and Graduate Level Education (continued)

- "Among the consequences [of a shortage of computer science researchers who concentrate in security areas] is that are a paucity of educational programs in security and a dearth of security experts." [NRC Computer Science and Telecommunications Board: *Trust in Cyberspace*, 1999, p. 235]

- "One of the nation's important shortcomings in our efforts to protect our critical infrastructures is a shortage of skilled information technology personnel … this shortage is acute when looking at information systems security specifically, and within the Federal government, this shortage amounts to a 'crisis …' " [John Tritak, Director of CIAO, testifying before the Senate Judiciary Committee's Subcommittee on Technology, Terrorism, and Government Information, on 6 Oct 99].

The State of Research and Development and Graduate Level Education (concluded)

- "American businesses, in an ever-shrinking and more highly competitive world, have devoted less and less of their precious resources to long-term R&D, directing their efforts instead to reducing costs and getting new products into the pipeline today at the expense of the future." [The President's Information Technology Advisory Committee (PITAC), 1999].

- "The training of future researchers is the most important thing that universities can do to ensure a strong *future* for basic research." [CED 1988].

EPILOGUE

- The trustworthiness of the risk assessment and management models developed for interdependent critical infrastructures will vary and their structure and scope will largely depend on:
    - The level of the decision-making for which they are intended to be used.
    - The temporal domain for which they are intended to be used.
    - The overlapping nature of the mission, mandate, responsibility, cooperation, and number of the involved organizations and agencies.
    - The quality, timeliness, and effectiveness of the flow of information facilitated among the concerned parties.

EPILOGUE (concluded)

- Understanding and modeling the physical and cyber interconnectedness and interdependencies among physical infrastructures is a daunting task. However, it is even more daunting when we attempt to map the flow of information among the organizational web and within the complex hierarchical decision-making process.

- To the extent that risk assessment is precise, it is not real.

  To the extent that risk assessment is real, it is not precise.

Backup Material

References

Automated software-based tools:

Kaplan, Stan, (1996), *An Introduction to TRIZ*, Ideation International, Inc. , Southfield, Michigan

General analytical risk tools and methods:

Ang, A. H. S., and W. H. Tang, 1984. *Probability Concepts in Engineering Planning and Design, Volume II: Decision, Risk, and Reliability*. Wiley, N.Y.

Asbeck, E., and Y. Y. Haimes, 1984. The Partitioned Multiobjective Risk Method, *Large Scale Systems* 6(1), 13-38.

Frohwein, H.I., J.H. Lambert, Y.Y. Haimes, and L.A. Schiff 1999. A multicriteria framework to aid the comparison of roadway improvement projects. *Journal of Transportation Engineering* 125(3):224-230.

Glickman, Theodore S. and M. Gough e.d. (1990), *Readings in Risk*, Johns Hopkins University Press, Washington D.C.

Haimes, Y. Y., 1998. *Risk Modeling, Assessment and Management*. Wiley, N.Y.

References (cont)

General analytical risk tools and methods (cont):

Haimes, Y.Y., 1988. Alternatives to the Precommensuration of Costs, Benefits, Risks, and Time in The Role of Social and Behavioral Sciences in *Water Resources Planning and Management*. D. D. Bauman and Y. Y. Haimes, editors, ASCE, New York.

Haimes, Y. Y., D. Li, P. Karlson, and J. Mitsiopoulus, 1990a. Extreme Event: Risk Management, in *System and Control Encyclopedia*, Supplementary Vol. 1. M. G. Singh, editor, Pergamon Press, Oxford.

Haimes, Y.Y., and C. Chittister, 1995. An Acquisition Process of Management of Non-Technical Risks Associated with Software Development, *Acquisition Review Quarterly* 11(2), 121-154.

Kaplan, S., et.al. 1999. *New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD™) and the Theory of Scenario Structuring*. Southfield, MI: Ideation International, Inc.

References (cont)

General analytical risk tools and methods (cont):

Kaplan, S. 1996. *An Introduction to TRIZ, the Russian Theory of Inventive Problem Solving.* Southfield, MI: Ideation International, Inc.

Kaplan, S. 1997. The Words of Risk Analysis, *Risk Analysis* 17, no. 4:407-417.

Kaplan, S. 1992. 'Expert Opinion' versus 'Expert Opinions'; Another Approach to the Problem of Eliciting/Combining/Using Expert Opinion in PRA, *Journal of Reliability Engineering and System Safety* 35:61-72.

Modarres,M., M. Kaminskiy, and V. Krivstov, 1999, *Reliability engineering and risk analysis,* New York : Marcel Dekker.

Moore, Peter G., (1983), *The Business of Risk*, Cambridge University Press, New York, NY

National Research Council, (1996), *Understanding Risk*, National Academy Press, Washington D.C.

References (cont)

General engineering tools:

Henley, Ernest J. and H. Kumamoto, (1992), *Probabilistic Risk Assessment*, IEEE Press, New York, NY

O'Connor, Patrick, D.T., (1985), *Practical Reliability Engineering*, Second ed., Heydon & Son Ltd., New York, NY

Domain-specific tools and methods:

B. Bush, R. Gordon, J. Holland, J. Fred Roach, D. Thompson, (1996), "The SOFIA Project for Interdependent Infrastructure Modeling, Simulation, and Analysis", LA-UR-99-3412, Los Alamos National Laboratory

Carnegie Mellon University/ Software Engineering Institute, (1995), " People Capability Maturity Model", CMU/SEI-95-M-02

Goodman G.T. and W.D. Rowe e.d. (1979), *Energy Risk Management*, Academic Press, New York, NY

References (cont)

Reliability tools and methods:

Blischke, W. R. and D.N. Prabhakar Murthy (2000) *Reliability : modeling, prediction, and optimization,* New York : John Wiley.

Rigdon, Steven E. and Asit P. Basu (2000) *Statistical methods for the reliability of repairable systems*, New York : Wiley.

Birolini, Alessandro (1999), *Reliability engineering : theory and practice* New York : Springer.

Thompson, G. (1999), *Improving maintainability and reliability through design.* London : Professional Engineering Publishing, 1999

Dodson, Bryan and D. Nolan (1999), Reliability engineering handbook, New York : Marcel Dekker.

Pyzdek, Thomas (1999), *Quality engineering handbook*, New York : Marcel Dekker.

References (cont)

Reliability tools and methods (cont.):

Modarres, M. (1999), *Reliability engineering and risk analysis*, New York : Marcel Dekker

Kales, P. (1998), Reliability for Technology, Engineering, and Management, Upper Saddle River, New Jersey: Prentice-Hall.

Leemis, Lawrence, M., (1995), *Reliability – Probabilistic Models and Statistical Methods*, Prentice-Hall Inc., Englewood Cliffs, NJ

Tobias, P. A. and D.C. Trindade (1995), *Applied Reliability*, Chapman & Hall/CRC

Hoyland, A. and M. Rausand (1993), *System Reliability Theory*, New York: John Wiley & Sons.

International Atomic Energy Agency, (1989), *Evaluating the Reliability of Predictions Made Using Environmental Transfer Models*, Safety Series No. l00, IAEA, Vienna

McCormick, Norman J., (1981), *Reliabilty and Risk Analysis*, Academic Press, New York, NY